CHAPTER XII I

PROGRAM MANAGEMENT

Section 1

EXECUTIVE BRANCH OVERSIGHT AND POLICY DIRECTION

13-100 National Security Council

Pursuant to the provisions of E. O. 12356 (reference (g)), the NSC shall provide overall policy direction for the Information Security Program.

13-101 Administrator of General Services

The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established under reference (g). In accordance with reference (g), the Administrator delegates the implementation and monitorship functions of the Program to the Director of the 1S00.

13-102 Information Security Oversight Office

a. Composition. The 1S00 has a full-time director appointed by the Administrator of General Services with approval of the President. The Director has the authority to appoint a staff for the office.

b. Functions. The Director of the 1S00 is charged with the following principal functions that pertain to the Department of Defense:

1. Oversee DoD actions to ensure compliance with reference (g) and implementing directives, for example, the 1S00 Directive No. 1 (reference (h)) and this Regulation;

2. Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the Information Security Program;

3. Report annually to the President through the NSC on the implementation of reference (g);

4. Review this Regulation and DoD guidelines for systematic declassification review; and

5. Conduct on-site reviews of the Information Security Program of each DoD Component that generates or handles classified information.

c. Information Requests. The Director of the 1S00 is authorized to request information or material concerning the Department of Defense, as needed by the 1S00 in carrying out its functions.

d. Coordination. Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the 1S00 are brought to the attention of the Director of Security Plans and Programs, ODUSD(P).

Section 2

DEPARTMENT OF DEFENSE

13-200 Management Responsibility

a. The DUSD(P) is the senior DoD official having DoD-wide authority and responsibility to ensure effective and uniform compliance with and implementation of E.O. 12356 and its implementing 1S00 Directive No. 1 (references (g) and (h)). As such, the DUSD(P) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The DUSD(P) or his designee may approve waivers or exceptions to the provisions of this Regulation to-the extent such action is consistent with references (g) and (h).

REQUEST FOR WAIVERS SHALL BE PREPARED FOR THE SIGNATURE OF THE DIRECTOR, WHS, AND ADDRESSED TO DUSD(P). BEFORE SUBMISSION FOR SIGNATURE, THE REQUEST SHALL BE COORDINATED WITH DIRECTOR, PSD.

b. The heads of DoD Components may approve waivers to the provisions of this Regulation only as specifically provided for herein.

REQUESTS TO THE DIRECTOR, WHS, FOR WAIVERS SHALL BE SIGNED BY THE HEAD OF THE OSD COMPONENT CONCERNED AND ROUTED THROUGH THE DIRECTOR, P'SD.

c. The Director, NSA/Chief, Central Security Service, under DoD Directive 5200.1 (reference (f)), is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. In this regard, the Director, NSA, may approve waivers or exceptions to these special requirements. Except as provided in subsection 1-205, the authority to lower any COMSEC security standards rests with the Secretary of Defense. Requests for approval of such waivers or exceptions to established COMSEC security standards which, if adopted, will have the effect of lowering such standards, shall be submitted to the DUSD(P) for approval by the Secretary of Defense.

Section 3

DOD COMPONENTS

13-300 General

The head of each DoD Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this Regulation throughout the Component.

13-301 Military Departments

In accordance with DoD Directive 5200.1 (reference (f)), the Secretary of each Military Department shall designate a senior official who shall be responsible for complying with and implementing this Regulation within the Department.

13-302 Other Components

In accordance with DoD Directive 5200.1 (reference (f)), the head of each other DoD Component shall designate a senior official who shall be responsible for complying with and implementing this Regulation within their respective Component.

a. THE DIRECTOR, WI-IS, IS THE SENIOR OFFICIAL RESPONSIBLE FOR THE INFORMATION SECURITY PROGRAM WITHIN OSD COMPONENTS.

b. THE OFFICIAL RESPONSIBLE FOR THE DAY-TO DAY IMPLEMENTATION OF THE INFORMATION SECURITY PROGRAM WITHIN OSD COMPONENTS IS THE DIRECTOR, PSD.

13-303 Program Monitorship

The senior officials designated under subsections 13-301 and 13-302 are responsible within their respective jurisdictions for monitoring, inspecting with or without prior announcement, and reporting on the status of administration of the DoD Information Security Program at all levels of activity under their cognizance.

13-304 Field Program Management

a. Throughout the Department of Defense, the head of each activity shall appoint, in writing, an official to serve as security manager for the activity. This official shall be responsible for the administration of an effective Information Security Program in that activity with particular emphasis on security education and training, assignment of proper classifications, downgrading and declassification, safeguarding, and monitorship, to include sampling classified documents for the purpose of assuring compliance with this Regulation.

THE HEADS OF OSD COMPONENTS SHALL:

1. IMPLEMENT THE SECURITY PROCEDURES AND INFORMATION SECURITY PROGRAM.

2. DESIGNATE, IN WRITING, PRIMARY AND ALTERNATE OFFICIALS WHO ARE TO SERVE AS SECURITY MANAGERS WITHIN THEIR RESPECTIVE COMPONENT AND PROVIDE A COPY OF THESE DESIGNATIONS TO THE DIRECTOR, PSD.

3. ENSURE THE SECURITY MANAGER IS EXPERIENCED IN WORKING WITH CLASSIFIED MATERIAL.

4. ASSIST THE SECURITY MANAGER IN COMPLYING WITH THIS INSTRUCTION .

b. Activity heads shall ensure that officials appointed as security managers either possess, or obtain within a reasonable time after appointment, knowledge of and training in the Information Security Program commensurate with the needs of their positions. The Director of Security Plans and Programs, ODUSD(P) shall, with the assistance of the Director, Defense Security Institute, develop minimum standards for training of activity security managers. Such training should result in appropriate certifications to be recorded in the personnel files of the individuals involved.

c. Activity heads shall ensure that officials appointed as security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They also shall provide sufficient resources of time, staff, and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of the Information Security Program at all levels of the activity.

THE OSD COMPONENT SECURITY MANAGER SHALL:

1. **ADVISE AND REPRESENT THE HEAD OF THE OSD COMPONENT ON MATTERS RELATED TO THIS INSTRUCTION.**

2. **ESTABLISH, IMPLEMENT, AND MAINTAIN AN EFFECTIVE SECURITY EDUCATION PROGRAM .**

3. **ESTABLISH PROCEDURES FOR ENSURING THAT ALL PERSONS HANDLING CLASSIFIED MATERIAL ARE CLEARED PROPERLY AND HAVE A NEED TO KNOW.**

4. **ENSURE THAT RESPONSIBLE OFFICIALS CREATE, REVIEW, AND UPDATE WHEN REQUIRED, CLASSIFICATION GUIDES FOR CLASSIFIED PLANS, PROGRAMS, AND PROJECTS.**

5. **ENSURE, IN COORDINATION WITH RECORDS MANAGEMENT PERSONNEL, THE REVIEW AND CONTINUAL REDUCTION OF CLASSIFIED INFORMATION WITH THE OSD COMPONENT BY DECLASSIFICATION, DESTRUCTION, OR RETIREMENT. RECORDS MANAGEMENT** PERSONNEL **SHALL OVERSEE THE OSD COMPONENT ANNUAL CLEAN-OUT DAYS.**

Section 4

INFORMATION REQUIREMENTS

13-400 Information Requirements

DoD Components shall submit on a fiscal year basis a consolidated report concerning the Information Security Program of the Component on SF 311, "Agency Information Security Program Data," to reach the ODUSD(P) by October 20 of each year. SF 311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the ODUSD(P). The ODUSD(P) shall submit the DoD report (SF 311) to the 1S00 by October 31 of each year. Interagency Report Control Number 0230-GSA-AN applies to this information collection system as well as to that contained in subsection 1-602.

Section 5

DEFENSE INFORMATION SECURITY COMMITTEE

13-500 Purpose

The Defense Information Security Committee (DISC) is established to advise and assist the DUSD(P) and the Director, Security Plans and Programs, ODUSD(P) in the formulation of DoD Information Security Program policy and procedures.

13-501 Direction and Membership

The DISC shall meet at the call of the DUSD(P) or the Director, Security Plans and Programs. It is comprised of the DUSD(P) as Chairman; the Director, Security Plans and Programs, as Vice Chairman; and the senior officials (designated in accordance with section E.3.a., DoD Directive 5200.1, reference (f)) (or their representatives) responsible for directing and administering the Information Security Program of the OJCS, the Departments of the Army, Navy, and Air Force, the Defense Intelligence Agency, the Defense Nuclear Agency, the National Security Agency, and the Defense Investigative Service. Other DoD Components may be invited to attend meetings of particular interest to them.